スマートフォンアプリ認証型
2段階認証構築システム
「AppCertify」 導入にあたって

カレット株式会社

1 App Certify使用者

Microsoft Authenticator、Google Authenticator、IIJ SmartKey、Authy 等の、ワンタイムパスワード管理アプリを予めスマートフォンにインストールしていただく必要がございます。

また、その管理アプリにApp Certifyを事前に登録していただく必要がございます。

2 App Certifyを導入するシステム

App Certify使用者が管理アプリにApp Certifyを登録するための画面（※後述：必要に応じ）と、2段階認証用入力画面の2種類の画面をご用意いただく必要がございます。

App Certifyを登録するためには、登録用QRコードをカメラから読み取る必要があるため、このQRコードを表示する画面が必要となりますが、システム接続図に記載の通り、一意な情報が必要となるため、例えば、ユーザー情報が閲覧できる画面などにQRコードやアプリへのリンク、そしてそれらの説明を記載すると、使用者はスムーズに進められるものと考えております。

※ただし、ログイン認証に2段階認証を挟む場合は、ログイン後のユーザー情報内の表示には適しておりませんので、使用者全員分のQRコードを予め発行し、一斉にお知らせするなど、別の方法をとる必要も出てまいります。これらケースに合わせ、提案させていただきます。

システム接続図

Caret

御社サーバー（サービスサイト）

弊社サーバー（API）

App Certify 登録画面

スマートフォンにインストールした Microsoft Authenticator等のアプリへ本システムを登録する画面。
例）ユーザー情報閲覧画面

変化しないシーケンシャルナンバーやユニークIDなどの一意な情報（もしくはそれらを非可逆暗号化した情報）をAPIに送信していただきます。

登録用QRコード表示API

APIが正常に呼び出されますと、アプリへ登録するためにスマートフォンのカメラから読み込むためのQRコード画像をバイナリー出力、もしくは、画像URLを返します。

2段階認証画面

自由なデザインで制作された1行テキスト入力画面 (デザイン指定等なし)。
ここにアプリで表示されたパスを入力。
例）ログイン後の重要な認証を必要とする場所

変化しないシーケンシャルナンバーやユニークIDなどの一意な情報（もしくはそれらを非可逆暗号化した情報）と入力されたパスワードをAPIに送信していただきます。

認証用API

送信いただいた一意な情報とパスワードを、本システム内で照合をかけ、成功もしくは失敗のステータスコードを返します。

注意
記載されている送信情報等は、セキュリティの観点から、あくまでも一例となります。
サーバーや導入システムにより、記載以上の情報の送受信が発生する場合がございます。予めご了承ください。

システム連携画面イメージ【ログイン画面で使用する場合】

Caret

1

下記QRコードが掲載されたURLを全ユーザーにメール等で連絡。
※URL・QRコードはユーザー毎に異なります。

下記QRコードを、Microsoft Authenticator, IIJ SmartKey, Google Authenticator 等のスマートフォンアプリで読み込み、本システムを追加してください。

https://aaa.aa/aa.php?aa=aaaaa
この画面は、御社サーバー・弊社サーバーどちらにでも設置可能です。

2

QRコードをアプリから読み込むと、App Certifyが追加されます。
※認証キーはユーザー毎に異なります。

Amazon
240 179

Google
476 325

Yahoo
897 358

Evernote
358 012

App Certify
757 017

6桁の認証キーは数十秒で新たに発行されます。

各ユーザー所有のスマートフォンアプリ画面

3

御社管理のサービスサイトにて、通常のID・パスワード認証を行います。

ID・パスワードを入力してください。

ID

パスワード

ログイン

https://bbb.bb/bb.bbb

4

御社管理のサービスサイトにて、ワンタイムパスワード認証を行います。
※認証には弊社サーバー(API)との連携が必須です。

スマートフォンアプリを開き、6桁のワンタイムパスワードを入力してください。

ワンタイムパスワード

認証

画面2のアプリを起動し、表示された認証キーを入力します。

この画面は、御社サーバー・弊社サーバーどちらにでも設置可能です。

画面3で認証が通った場合、画面4の認証キーとユーザー情報を紐づけるため、例えばIDをハッシュ化した情報等のパラメータを付与し画面4を呼び出していただく必要がございます。

システム連携画面イメージ【ログイン画面でAPI連携なしの場合】

Caret

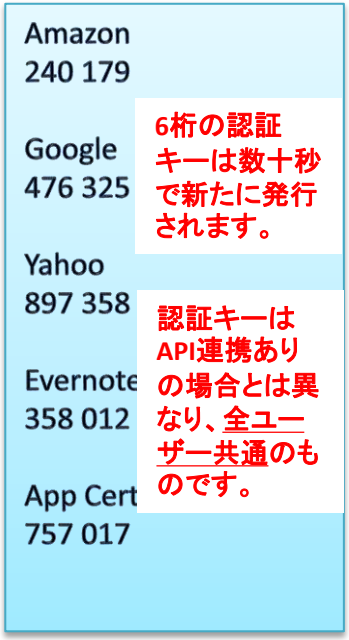
1

下記QRコードが掲載されたURLを全ユーザーにメール等で連絡。
※URL・QRコードは全ユーザー同一のものとなります。

https://aaa.aa/aa.php
この画面は、御社サーバー・弊社サーバーどちらにでも設置可能です。

2

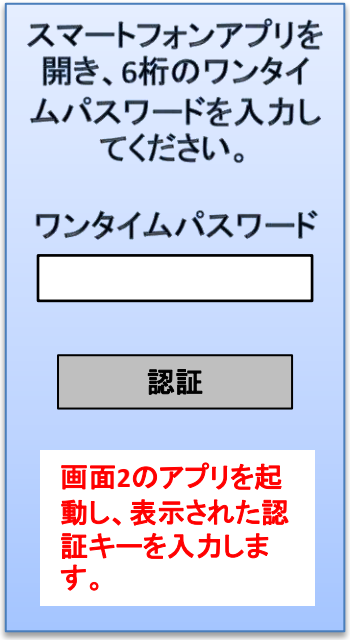
QRコードをアプリから読み込むと、App Certifyが追加されます。
※認証キーは全ユーザー同一のものとなります。



各ユーザー所有の
スマートフォンアプリ画面

3

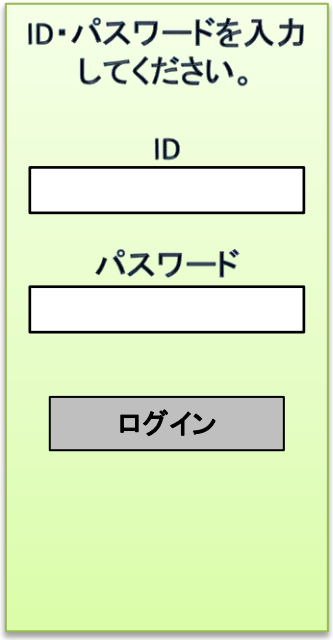
御社管理のサービスサイトにて、ワンタイムパスワード認証を行います。
※認証での弊社サーバー(API)との連携は不要です。



この画面は、御社・弊社サーバーどちらにでも設置可能ですが、完全に連携不要にする場合は弊社サーバー(リダイレクト型)となります。

4

御社管理のサービスサイトにて、通常のID・パスワード認証を行います。



https://bbb.bb/bb.bbb

画面3で認証が通った場合、画面4には御社より指定された形式でのパラメータ(例:日時+〇〇をハッシュ化した値、等、システム内でしかわからないルールに従ったもの)を付与し画面4へリダイレクトしますので、そのパラメータにて認証の合否判定を行ってください。

API連携した場合のメリット・デメリット

メリット
・ユーザー単位で異なる認証キーが発行されるため、セキュリティレベルが非常に高い。
・ユーザー1人のQRコードが漏洩した場合であっても、1人分の再発行で問題がない。
※漏洩しても前段となるID・パスワード認証があるため、それを突破できない限りは
特にトラブルに発展することはない。

デメリット
・既存システムとの連携が必須となるため、既存システムの改修が必須となる。

API連携しない場合のメリット・デメリット

メリット
・既存システムとのAPI連携がなくなるため、既存システムの改修が不要となる。

デメリット
・社内全ユーザー共通の認証キーが発行されるため、セキュリティレベルが低くなる。
・そのため、定期的なQRコードの再発行・アプリへの再登録をするという運用が望ましい。
※漏洩してもその後のID・パスワード認証があるため、それを突破できない限りは
特にトラブルに発展することはない。2要素認証の補助的な役割としての色が濃い。

一切御社システムの変更ができない場合の案

概要説明

・P4の4にある御社システムが導入されているルート配下に.htaccess・.htpasswdを設置し、Basic認証をかけます。
・P4の3で認証が通った際の御社システムへのリダイレクト時に、Authorizationヘッダー付与やURL内認証情報付与等でこのBasic認証情報を含ませ、御社システムにかかったBasic認証を通過させます。
これにより、P4の4にダイレクトにアクセスした場合、Basic認証を通過させることができないため、エラーとなります。
・セキュリティをさらに強化したい場合、毎日このBasic認証情報を変更するシステムの開発も弊社にて可能です。

メリット・デメリット

メリット
・既存システムとの連携が一切なくなるため、既存システムの改修が不要となる。
・内部的には3要素認証となるため、社内全ユーザー共通の認証キーが発行されるものの、セキュリティレベルは高い。
デメリット
・ワンタイムパスワード単体で言えば、API連携型と比較すればセキュリティレベルは低い。
ただし前述の通り、それ以上のセキュリティが新たに加わるため、単純な比較にはならない。

本案の必要条件

・御社システム内プログラムに対する改修は一切必要ございません。
・Basic認証を御社システム全体にかけるため、御社システムが導入されているドキュメントルート領域に、.htaccess・.htpasswdを設置させていただくことが必須となります。
・セキュリティをさらに強化するため、毎日このBasic認証情報を変更するシステムも弊社にて開発可能でございますが、御社サーバーのcrontabに、弊社開発のPHPプログラムを定期起動するよう設定させていただくことが必須となります。

一切御社システムの変更ができない場合の案：画面イメージ

Caret

1

下記QRコードが掲載されたURLを全ユーザーにメール等で連絡。
※URL・QRコードは全ユーザー同一のものとなります。

https://aaa.aa/aa.php
この画面は、御社サーバー・弊社サーバーどちらにでも設置可能です。

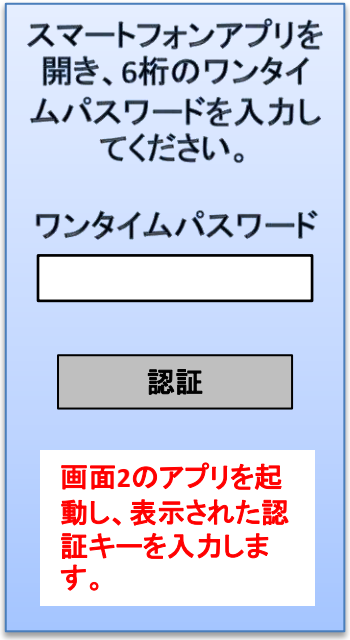
2

QRコードをアプリから読み込むと、App Certifyが追加されます。
※認証キーは全ユーザー同一のものとなります。

各ユーザー所有の
スマートフォンアプリ画面

3

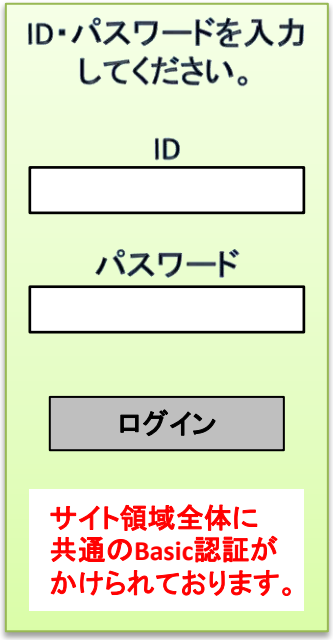
御社管理のサービスサイトにて、ワンタイムパスワード認証を行います。
※認証での弊社サーバー(API)との連携は不要です。



この画面は、御社・弊社サーバーどちらにでも設置可能ですが、完全に連携不要にする場合は弊社サーバー(リダイレクト型)となります。

4

御社管理のサービスサイトにて、通常のID・パスワード認証を行います。



https://bbb.bb/bb.bbb

画面3で認証が通った場合、画面4にはBasic認証を通過するためBasic認証のID・パスワードが付与された状態で画面4へリダイレクトしますので、画面3の認証通過と同時に自動的にBasic認証を突破されている状態となっております。よって、画面3を通さず画面4にダイレクトアクセスした場合は、Basic認証ダイアログが出るため、アクセス失敗となります。